PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K	A2	**(11) International Publication Number:** WO 95/14283 **(43) International Publication Date:** 26 May 1995 (26.05.95)

(21) International Application Number: PCT/US94/12426

(22) International Filing Date: 28 October 1994 (28.10.94)

(30) Priority Data:
148,716 8 November 1993 (08.11.93) US

(71) Applicant: HUGHES AIRCRAFT COMPANY [US/US]; 7200 Hughes Terrace, Los Angeles, CA 90045 (US).

(72) Inventors: BATHRICK, Erwin, W.; 315 East Blossom Place, Brea, CA 92621 (US). GARBER, John, W.; 691 Santa Maria Lane, Davidsonville, MD 21035 (US). HUANG, Cheng-Chi; 7 Mountain Ash, Irvine, CA 92714 (US). KUNG, Kenneth, C.; 19029 Vickie Avenue, Cerritos, CA 90701 (US). MATTHEWS, Todd, E.; 2508 Jacaranda Street, Santa Ana, CA 92701 (US). ZUMDA, James, E.; 22136 Elsberry Way, Lake Forest, CA 92630 (US). MATTHEWS, Regina, L.; 5260 Avenida Despacio, Yorba Linda, CA 92687 (US).

(74) Agents: WALDER, Jeannette, M. et al.; Hughes Aircraft Company, P.O. Box 80028, Building C1, M/S A126, Los Angeles, CA 90080-0028 (US).

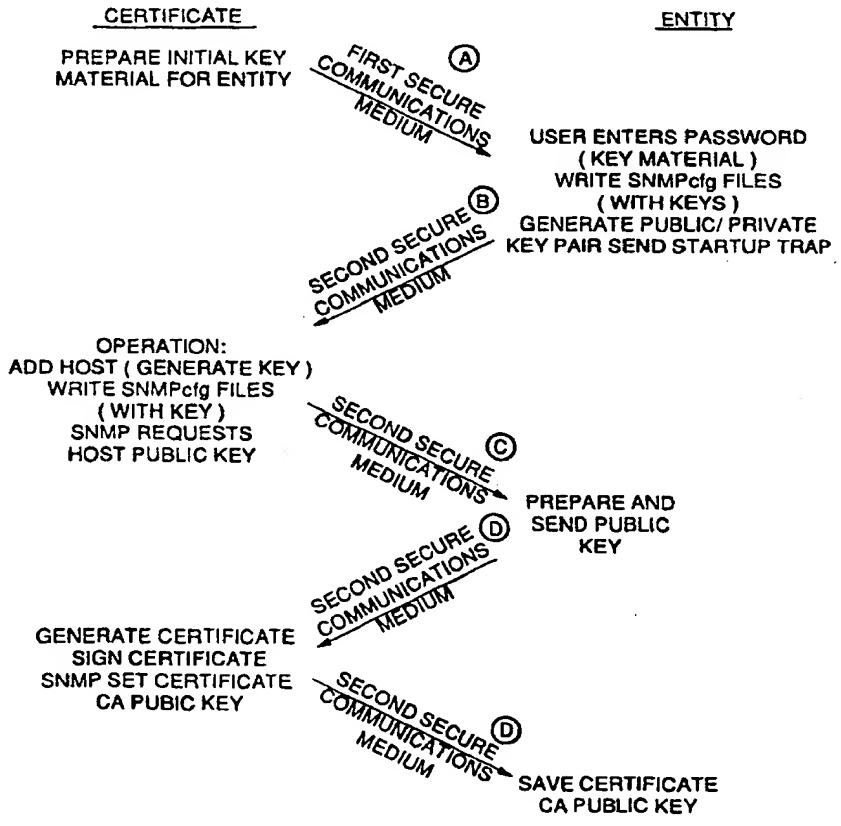
(81) Designated States: AU, CA, JP, KR, NO, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: PROTECTED DISTRIBUTION PROTOCOL FOR KEYING AND CERTIFICATE MATERIAL

(57) Abstract

Disclosed is a computer system and a method for the protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain, comprising the steps of sending keying material, including a password, generated by the Certifying Authority to the entity via a secure medium; generating and protecting, by the entity, a public and a private key pair using the keying material provided it by the certifying authority; generating, protecting and sending a request for a certificate to the certifying authority using the keying material provided it by the certifying authority; requesting, by the certifying authority, that the public key and address of the entity be sent to the certifying authority; protecting and sending the public key and address of the entity to the certifying authority using the keying material provided it by the certifying authority; assembling and issuing the certificate to the entity from the certifying authority and recording the public key of the entity at the certifying authority for public use within the domain of the certifying authority.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

PROTECTED DISTRIBUTION PROTOCOL FOR KEYING AND CERTIFICATE MATERIAL

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates in general to computer security systems, and, more particularly, to a computer security system and a method for the protected distribution of certificate and keying material between a certification authority and an entity in the certification authority's domain.

2. Description of the Related Art

In existing methods for distribution of certificate and keying material, the administrator must manually distribute the information to each end system (entity) and user. Administrators in the past were required to visit each system or user on the system more than once to initialize the information required to support the network security mechanism.

The certificate or keying material is used later to authenticate and to protect the communications between distributed entities. If these materials are compromised in the initial distribution, then the confidentiality and authentication services cannot be assured during further operation.

This manual distribution system is further fraught with difficulties in maintaining security in the physical transportation of the keying materials between the Certification Authority and the various entities, and with the consequent time lag mandated by the actual wait times involved in moving from one entity to the other. All during this setup time, the various entities are denied access to the protected data for which they may have an immediate need.

The present invention meets and overcomes this problem of maintaining security during the transfer of the keying

materials between entities and shortens the time during which access is denied an otherwise authorized entity to a minimum.

The present invention reduces the required visits needed to install the necessary security access software to a single visit by using a password (shared secret) to generate the essential keying material to be used for both integrity and encryption services to protect the data necessary for authentication and network security protocol protection.

OBJECTS AND SUMMARY OF THE INVENTION

Therefore, it is an object of the present invention to provide a computer security network system and a method for the protected distribution of certificate and keying material between a certification authority and an entity in the certification authority's domain.

It is still another object of the present invention to provide a method and system that quickly provides authorized users control of their data.

It is another object of the present invention to provide a method and system that facilitates, rather than prevents, the establishment of encoded public and private key data or documents classified at different security levels.

The present invention provides a computer system and a method for the protected distribution of certificate and keying material between a certification authority and an entity in the certification authority's domain by establishing a shared secret and using it to protect the data transferred between the entity and the certifying authority.

The novel features of construction and operation of the invention will be more clearly apparent during the course of the following description, reference being had to the accompanying drawings wherein has been illustrated a preferred form of the device of the invention and wherein

like characters of reference designate like parts throughout the drawings.

BRIEF DESCRIPTION OF THE FIGURES

FIGURE 1 is a block diagram flowchart showing the general overall logic flow through a system incorporating the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENT

A preferred form of the invention as embodied in a method and computing system for providing for the protected distribution of certificate and keying material between a certification authority and an entity in the certification authority's domain by establishing a shared secret and using it to protect the data transferred between the entity and the certifying authority.

In general, as shown in FIGURE 1, the invention is found in a computer system operating over a network in accord with the following steps outlined below in detail to provide for the protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain.

The certifying authority begins by generating and sending keying material, including a password, to the subject entity via a first secure communications medium. In this instance, the most secure communications medium is a non-electronic medium, such as a manual courier, secure mail or other secure communications medium that is distinct from the computer system over which the keying material is to be used as described later in authenticating the entity to the certifying authority.

Once the entity receives the keying material from the certifying authority, it then generates a public and a private key pair and protects the public key using the keying material provided it by the certifying authority.

The entity now generates and protects a request for a certificate to the certifying authority by using the keying

material provided it by the certifying authority. Once generated and protected, the request is sent to the certifying authority via a second secure communications medium connecting the certifying authority with the entities in its certifying domain.

Once the certifying authority receives the request from the entity, the certifying authority authenticates the identity of the requesting entity. This is done by requesting, via the second secure communications medium, that the public key and address of the entity be sent to the certifying authority.

The requesting entity, having received the authentication request from the certifying authority, protects the transmission of its selected public key and address to the certifying authority via the second secure communications medium, by using the keying material provided by the certifying authority.

Once the identity of the requesting entity is confirmed, the certifying authority then assembles and issues the requested certificate to the entity via the second secure communications medium, and records the public key of the entity at the certifying authority for public use by other entities within the certifying domain of the certifying authority.

The invention described above is, of course, susceptible to many variations, modifications and changes, all of which are within the skill of the art. It should be understood that all such variations, modifications and changes are within the spirit and scope of the invention and of the appended claims. Similarly, it will be understood that Applicant intends to cover and claim all changes, modifications and variations of the example of the preferred embodiment of the invention herein disclosed for the purpose of illustration which do not constitute departures from the spirit and scope of the present invention.

WHAT IS CLAIMED IS:

1. A method for the protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain via a communications medium connecting the certification authority and entities in its domain, comprising the steps of:

sending keying material, including a password, generated by the certifying authority to the entity via a first secure communications medium;

generating and protecting, by the entity, a public and a private key pair using the keying material provided the entity by the certifying authority;

generating, protecting and sending via a second secure communications medium a request for a certificate to the certifying authority using the keying material provided the entity by the certifying authority;

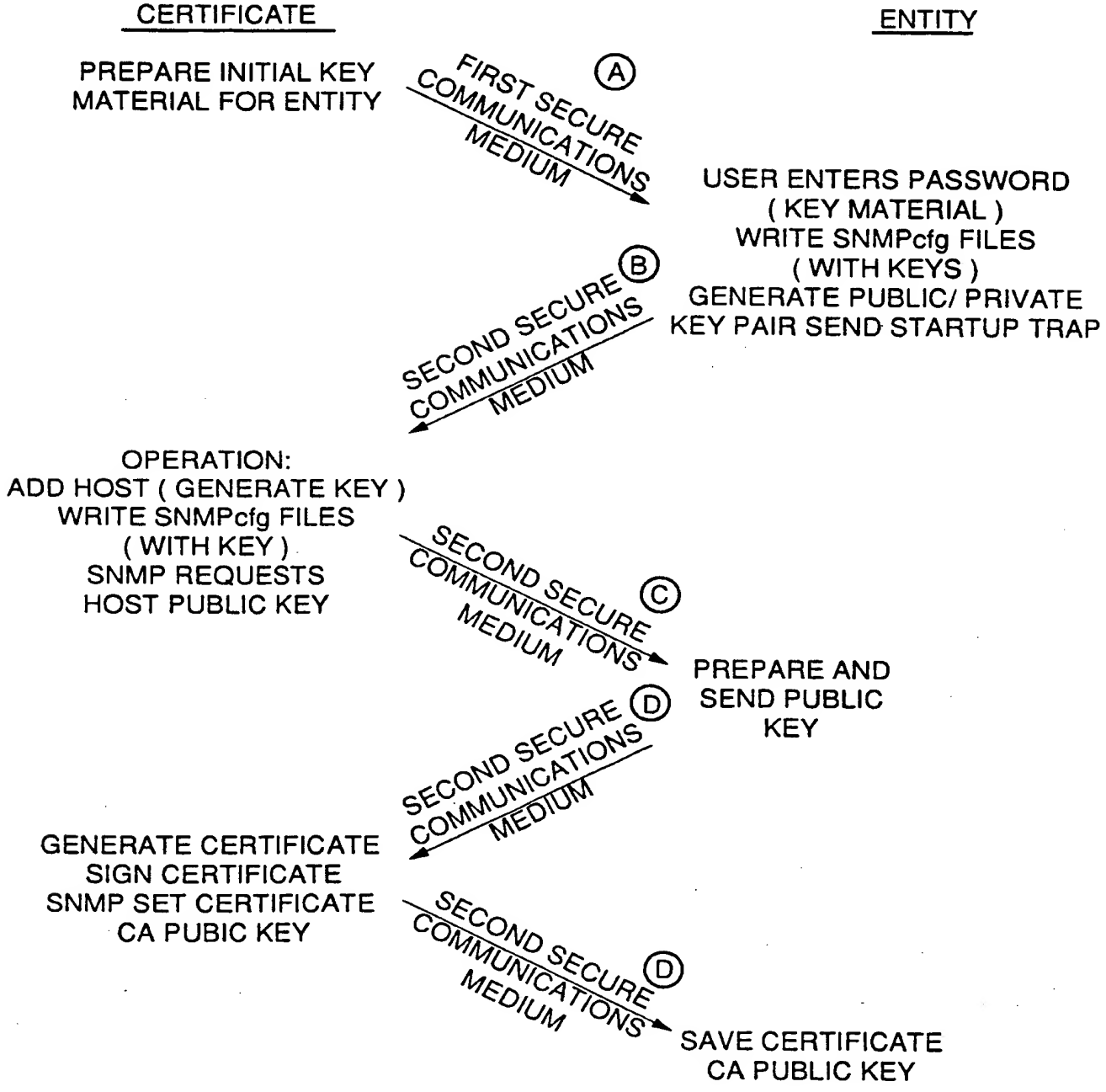
requesting, by the certifying authority via the second secure communications medium, that the public key and address of the entity be sent to the certifying authority;

protecting and sending the public key and address of the entity to the certifying authority via the second secure communications medium using the keying material provided it by the certifying authority;

assembling and issuing the certificate to the entity from the certifying authority via the second secure communications medium and recording the public key of the entity at the certifying authority for public use within the domain of the certifying authority.

2. The method of claim 1 wherein said step of sending keying material, including a password, generated by the certifying authority to the entity via a first secure communications medium further includes the step of: selecting the first secure communications medium that is separate and independent from the second secure communications medium.

3. The method of claim 1 wherein said step of sending keying material, including a password, generated by the certifying authority to the entity via a first secure communications medium further includes the step of: selecting a non-electronic transmission medium for the first secure communications medium.


CERTIFICATE
ENTITY
PREPARE INITIAL KEY MATERIAL FOR ENTITY
A
FIRST SECURE COMMUNICATIONS MEDIUM
USER ENTERS PASSWORD (KEY MATERIAL)
WRITE SNMPcfg FILES (WITH KEYS)
GENERATE PUBLIC/ PRIVATE KEY PAIR SEND STARTUP TRAP
B
SECOND SECURE COMMUNICATIONS MEDIUM
OPERATION:
ADD HOST (GENERATE KEY)
WRITE SNMPcfg FILES (WITH KEY)
SNMP REQUESTS HOST PUBLIC KEY
SECOND SECURE COMMUNICATIONS MEDIUM
C
PREPARE AND SEND PUBLIC KEY
D
SECOND SECURE COMMUNICATIONS MEDIUM
GENERATE CERTIFICATE
SIGN CERTIFICATE
SNMP SET CERTIFICATE
CA PUBIC KEY
SECOND SECURE COMMUNICATIONS MEDIUM
D
SAVE CERTIFICATE CA PUBLIC KEY

PCT WORLD INTELLECTUAL PROI International I

INTERNATIONAL APPLICATION PUBLISHED UNDE WO 9514283A3

(51) International Patent Classification 6 : **H04L 9/32, 9/08** | **A3**

(11) International Publication Number: **WO 95/14283**

(43) International Publication Date: 26 May 1995 (26.05.95)

(21) International Application Number: PCT/US94/12426

(22) International Filing Date: 28 October 1994 (28.10.94)

(30) Priority Data:
148,716 8 November 1993 (08.11.93) US

(71) Applicant: HUGHES AIRCRAFT COMPANY [US/US]; 7200 Hughes Terrace, Los Angeles, CA 90045 (US).

(72) Inventors: BATHRICK, Erwin, W.; 315 East Blossom Place, Brea, CA 92621 (US). GARBER, John, W.; 691 Santa Maria Lane, Davidsonville, MD 21035 (US). HUANG, Cheng-Chi; 7 Mountain Ash, Irvine, CA 92714 (US). KUNG, Kenneth, C.; 19029 Vickie Avenue, Cerritos, CA 90701 (US). MATTHEWS, Todd, E.; 2508 Jacaranda Street, Santa Ana, CA 92701 (US). ZUMDA, James, E.; 22136 Elsberry Way, Lake Forest, CA 92630 (US). MATTHEWS, Regina, L.; 5260 Avenida Despacio, Yorba Linda, CA 92687 (US).

(74) Agents: WALDER, Jeannette, M. et al.; Hughes Aircraft Company, P.O. Box 80028, Building C1, M/S A126, Los Angeles, CA 90080-0028 (US).

(81) Designated States: AU, CA, JP, KR, NO, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

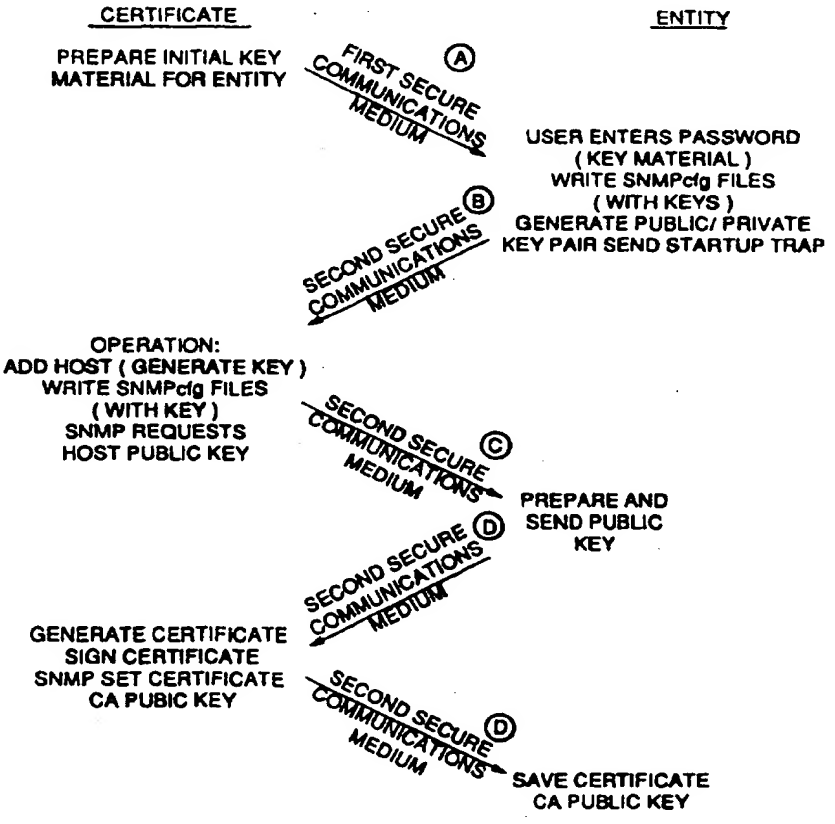
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report: 14 March 1996 (14.03.96)

(54) Title: PROTECTED DISTRIBUTION PROTOCOL FOR KEYING AND CERTIFICATE MATERIAL

(57) Abstract

Disclosed is a computer system and a method for the protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain, comprising the steps of sending keying material, including a password, generated by the Certifying Authority to the entity via a secure medium; generating and protecting, by the entity, a public and a private key pair using the keying material provided it by the certifying authority; generating, protecting and sending a request for a certificate to the certifying authority using the keying material provided it by the certifying authority; requesting, by the certifying authority, that the public key and address of the entity be sent to the certifying authority; protecting and sending the public key and address of the entity to the certifying authority using the keying material provided it by the certifying authority; assembling and issuing the certificate to the entity from the certifying authority and recording the public key of the entity at the certifying authority for public use within the domain of the certifying authority.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 94/12426

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY., vol. 11, no. 2, April 1992 AMSTERDAM NL, pages 173-183, XP 000245841 R.LAUN 'ASYMMETRIC USER AUTHENTICATION' see figures 1,3 see page 178, right column, line 23 - page 179, left column, line 10 see page 178, left column, line 5 - line 27 see page 177, left column, line 34 - right column, line 28 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 January 1996	12.02.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Authorized officer Lydon, M

Form PCT/ISA/210 (second sheet) (July 1992)

Inte onal Application No
PCT/US 94/12426

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 723 284 (MUNCK ET AL.) 2 February 1988 see column 3, line 52 - column 4, line 36 see column 5, line 44 - line 62 see figure 1 -----	1

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/US 94/12426

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-4723284	02-02-88	NONE	